

⑯ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑯ Offenlegungsschrift
⑯ DE 40 10 094 A 1

⑯ Int. Cl. 5:
G 06 F 12/14

DE 40 10 094 A 1

⑯ Aktenzeichen: P 40 10 094.4
⑯ Anmeldetag: 29. 3. 90
⑯ Offenlegungstag: 2. 10. 91

⑯ Anmelder:
Standard Elektrik Lorenz AG, 7000 Stuttgart, DE

⑯ Erfinder:
Martin, Georg, Dipl.-Ing., 7257 Ditzingen, DE

⑯ Verfahren zur Überprüfung der Zugangsberechtigung eines Benutzers zu einem Prozeß

⑯ Beschrieben wird ein Verfahren zur Überprüfung der Zugangsberechtigungen des Benutzers eines Datenverarbeitungsnetzes zu einem daran angeschlossenen Prozeß. Im Datenverarbeitungsnetz ist ein Authentifizierungsrechner (ATH) vorgesehen, zu dem ein den Zugang zu einem Prozeß anfordernder Benutzer mit einem ihm zugeordneten Passwort Zugang erhält. Der Authentifizierungsrechner erzeugt bei Anforderung durch den Benutzer einen Schlüssel (SL). Der Schlüssel (SL) enthält eine Benutzermaske (BENMAS), die angibt, zu welchen der an das Datenverarbeitungsnetz angeschlossenen Prozesse der anfordernde Benutzer eine Zugangsberechtigung hat. Dieser Schlüssel wird an den anfordernden Benutzer - ggf. kodiert - zurückübertragen. Unter Verwendung dieses Schlüssels steuert der Benutzer dann den von ihm gewünschten Prozeß an. In dem Prozeß wird die Benutzermaske (BENMAS) aus dem Schlüssel (SL) und aus der Benutzermaske die Zugangsberechtigung des anfordernden Benutzers festgestellt.

DE 40 10 094 A 1

BEST AVAILABLE COPY

Beschreibung

Die Erfindung betrifft ein Verfahren zur Überprüfung der Zugangsberechtigung eines Benutzers eines Datenverarbeitungsnetzes zu einem daran angeschlossenen Prozeß unter Benutzung eines Passwortes.

Es ist üblich, daß ein an ein Datenverarbeitungsnetz angeschlossener Benutzer für jeden Prozeß ein gesondertes Passwort braucht. Jeder an ein Netz angeschlossene Benutzer hat also meist mehrere Passworte, nämlich so viele wie er Zugangsberechtigungen zu unterschiedlichen Prozessen hat. Die Gültigkeit der Passworte ist üblicherweise zeitlich limitiert (1 bis 3 Monate). Nach Ablauf dieser Zeit wird vom Benutzer die Festlegung eines neuen Passwortes verlangt, ohne die Berechtigung neu zu prüfen. Dies führt dazu, daß man einfache Passworte sucht (Geburtstag der Ehefrau, Namen der Kinder, usw.). Es besteht auch die Gefahr, daß die Benutzer Notizen über Passworte an leicht zugänglichen Stellen (z. B. auf der Unterseite des Keyboards) aufbewahren. Damit wird die Sicherheitsfunktion der Passworte zu nichts gemacht.

Ein weiterer Nachteil der Anforderung des Zugangs zu einem bestimmten Prozeß über ein Datenverarbeitungsnetz mittels eines Passworts besteht darin, daß das Passwort selbst Gegenstand des Datenverkehrs auf dem Netz ist. Jeder, der überhaupt über einen Anschluß zu dem Netz verfügt oder ihn sich verschaffen kann (Hacker), kann also den Datenverkehr analysieren und daraus u. U. das Passwort gewinnen.

Ein weiterer Nachteil bekannter Systeme zur Zugangsaufrechterhaltung und Berechtigungsverwaltung besteht darin, daß die Zugangsberechtigung zeitlich unbegrenzt ist. Sie besteht für ausgeschiedene Mitarbeiter meist weiter; dasselbe gilt für Mitarbeiter, die eine bestimmte Zugangsberechtigung nicht mehr benötigen. Um die Zugangsmöglichkeit zu beenden, muß in den betroffenen Prozessen die Berechtigung gelöscht werden.

Aufgabe der Erfindung ist es daher, den Zugang zu mehreren verschiedenen Prozessen eines Datenverarbeitungsnetzes zu vereinfachen und gleichzeitig die Sicherheit gegen unbefugte Benutzung zu erhöhen.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, daß im Datenverarbeitungsnetz ein Authentifizierungsrechner vorgesehen ist, zu dem ein den Zugang zu einem Prozeß anfordernder Benutzer mit ihm zugeordneten bestimmten Passwort Zugang erhält, daß der Authentifizierungsrechner einen bestimmten Schlüssel für den Benutzer erzeugt, daß der Schlüssel eine Benutzermaske enthält, die angibt, zu welchen der an das Datenverarbeitungsnetz angeschlossenen Prozesse der anfordernde Benutzer eine Zugangsberechtigung hat, daß dieser Schlüssel an den anfordernden Benutzer zurückübertragen wird, und daß der Benutzer unter Verwendung dieses Schlüssels den von ihm gewünschten Prozeß ansteuert, daß dann in dem Prozeß die Benutzermaske aus dem Schlüssel und aus der Benutzermaske die Zugangsberechtigung des anfordernden Benutzers festgestellt und, falls vorhanden, diesem der Zugang zu dem Prozeß freigegeben wird.

Vorteilhafte Weiterbildungen der Erfindung sind in den Unteransprüchen definiert. Insbesondere ergibt sich unter Verwendung auch der genannten Weiterbildungen ein Verfahren, bei dem ein vom Authentifizierungsrechner erzeugter kodierter Schlüssel für jeden Benutzer eine Benutzermaske generiert, aus der die Prozesse ersichtlich sind, zu denen dieser Benutzer eine

Zugangsberechtigung hat. Ferner kann man vorteilhaftweise die Netzadresse des anfordernden Benutzers, das Benutzerdatum und die Dauer der Zugangsberechtigung in den Schlüssel mit einbeziehen. Diese Information wird kodiert an den anfordernden Benutzer zurückgegeben, der sich seinerseits damit den Zugang zu den Prozessen, für die er tatsächlich eine Zugangsberechtigung hat, verschaffen kann. Dies geht dann aber nur von einer bestimmten Netzadresse aus, an einem bestimmten Datum und für eine bestimmte Dauer.

10 Damit können alle Zugangsberechtigungen eines bestimmten Benutzers zentral verwaltet und jederzeit geändert werden, ohne daß damit irgendwelche Benutzerberechtigungen in den Prozessen geändert werden müssen. Der Benutzer braucht nur ein Passwort, nämlich das, das ihm den Zugang zu dem Authentifizierungsrechner verschafft.

15 Die Erfindung schafft also ein außerordentlich einfaches System der Zugangsaufrechterhaltung und Berechtigungsverwaltung mit erhöhter Sicherheit.

20 Ein Ausführungsbeispiel der Erfindung wird im folgenden unter Bezugnahme auf die beigefügten Zeichnungen näher beschrieben. Es stellen dar:

25 Fig. 1 ein Datenverarbeitungsnetz mit einem angeschlossenen Benutzer und verschiedenen angeschlossenen Prozessen;

Fig. 2 eine matrixförmig aufgebaute Liste, die die Zugangsberechtigungen einzelner Benutzer enthält;

30 Fig. 3 einen vom Authentifizierungsrechner erstellten Schlüssel;

Fig. 4 ein Ablaufplan für die Erstellung des Schlüssels im Authentifizierungsrechner;

Fig. 5 ein Ablaufplan für die Freigabe eines Prozesses unter Verwendung des Schlüssels.

35 Fig. 1 zeigt einen Ausschnitt aus einem Datennetz, an das ein Benutzer und verschiedene Prozesse, im Beispiel die Prozesse 1 bis 4, abgekürzt: Proz. 1, Proz. 2, Proz. 3, Proz. 4, angeschlossen sind.

40 An das Datenverarbeitungsnetz ist ferner ein Authentifizierungsrechner ATH angeschlossen. In diesem sind die Zugangsberechtigungen aller Benutzer in Form einer Matrix niedergelegt, wie dies aus Fig. 2 ersichtlich ist. Der Benutzer A hat z. B. für die Prozesse Proz. 2 und Proz. 3 eine Berechtigung, jeweils angezeigt durch eine "1", jedoch keine Berechtigung für die Proz. 1 und Proz. 4. Der Benutzer B hingegen hat eine Berechtigung für die Prozesse Proz. 1 und Proz. 2, nicht jedoch für die Prozesse Proz. 3 und Proz. 4.

45 Die Bits einer Zeile, also für den Benutzer A die Folge 0110, ist die Benutzermaske BENMAS dieses Benutzers.

50 Der Aufbau eines Schlüssels SL, der im Authentifizierungsrechner ATH generiert wird, ergibt sich aus Fig. 3. Die verschiedenen Benutzer haben an der Stelle, von der aus sie den Zugang zu einem bestimmten Prozeß haben wollen, also an ihrem Arbeitsterminal oder ihrer Workstation, eine bestimmte Netzadresse NETADR. Auch diese Netzadresse NETADR wird in den Schlüssel mit einbezogen. Das bedeutet, daß der Zugang zu dem Prozeß auch nur von dieser Netzadresse NETADR aus erlangt werden kann. Außerdem erhält der Schlüssel SL noch das Datum der Benutzung BENDAT. Nur für diesen Tag wird also ein Schlüssel erzeugt. Schließlich enthält der Schlüssel SL noch die Benutzungsdauer BEN-DAU. Nur für diese Zeit, z. B. halbe-Tage-weise oder für einige Stunden, gilt dann der Schlüssel SL. Ist diese Zeit abgelaufen, muß erneut ein Schlüssel generiert werden.

55 Wie aus Fig. 3 ersichtlich, wird also ein Schlüssel SL im Beispiel durch die Benutzermaske BENMAS, die

Netzadresse NETADR des Benutzers, das Datum der Anforderung BENDAT und die Benutzungsdauer BENDAU gebildet. Dieser Schlüssel SL wird im Authentifizierungsrechner ATH auf Anforderung erzeugt, kodiert und dann als kodierter Schlüssel KSL dem anfordernden Benutzer zurückübermittelt. Dieser kann sich damit Zugang zu den Prozessen, zu denen er eine Zugangsbe- 5
rechtigung besitzt (die also in der Benutzermaske BENMAS enthalten ist), beschaffen, und zwar nur von der Netzadresse NETADR aus, von der er aus den Schlüssel 10 angefordert hat, an dem Datum BENDAT, an dem die Anforderung und die Vergabe des Schlüssels KSL erfolgte, und ferner für die ebenfalls im kodierten Schlüssel KSL enthaltene Dauer BENDAU.

Der Ablauf der Erzeugung des Schlüssels SL bzw. des 15
kodierten Schlüssels KSL im Authentifizierungsrechner ATH ergibt sich aus Fig. 4. Im ersten Schritt schaltet sich der anfordernde Benutzer unter Nennung seines Namens (Username) und seines Passwortes im Authentifizierungsrechner ATH ein (LOGIN). Das Passwort, 20
das er dabei verwendet, ist das sein persönliches Passwort, das für ihn gilt. Jeder Benutzer hat also nur ein Passwort; es kann dementsprechend durchaus kompliziert sein. Unter Verwendung dieses nur einen Passworts erreicht der Benutzer ein LOGIN im Authentifizierungsrechner ATH. Das Passwort wird geprüft. Wenn 25
es gültig ist, wird für den Benutzer eine Berechtigungs- maske BENMAS aus der im Authentifizierungsrechner ATH gespeicherten Liste von Berechtigungen generiert. Es wird ferner die Netzadresse NETADR des an- 30
fordernden Benutzers ermittelt. Dies kann unter Benüt-
zung herkömmlicher Techniken erfolgen, etwa in glei-
cher Weise, wie im Fernschreib-Verkehr oder im Tele-
fax-Verkehr eine Kennung (ggf. Anschlußnummer) des 35
Anrufenden bei Anrufer erscheint. Ferner wird das Da-
tum der Benutzung BENDAT und die Berechtigungs-
dauer BENDAU erzeugt. Die Berechtigungsmaske BENMAS, Netzadresse NETADR des Anrufenden, Ben-
utzungsdatum BENDAT und Benutzungsdauer BENDAU werden dann zu einem Schlüssel SL verknüpft; 40
siehe Fig. 3. Nach einem Code, der auch wechseln kann,
wird aus diesem Schlüssel SL ein kodierter Schlüssel KSL erzeugt. Dieser wird an den anfordernden Benutzer zurückübertragen.

Wie aus Fig. 5 ersichtlich, kann dann sich der Benutzer 45
unter Verwendung dieses kodierten Schlüssels KSL und ferner unter Verwendung seines Namens Username bei einem bestimmten Prozeß einschalten, d. h. ein LOGIN vornehmen. Dort wird der Schlüssel dekodiert und wiederum Benutzermaske BENMAS, Netzadresse 50
NETADR, das Datum BENDAT, und die Benutzerdauer BENDAU ermittelt. Im nächsten Schritt wird geprüft, ob die Benutzermaske BENMAS eine Zugangsberechtigung für den aufgerufenen Prozeß enthält. Dies ergibt sich aufgrund der in dem Prozeß niedergelegten Be- 55
rechtigungen analog zur Liste der Berechtigungen in Fig. 2. Außerdem wird die Adresse NETADR des dem Zugang zu diesem Prozeß anfordernden Benutzers er-
mittelt. Ist die Adresse gleich der Netzadresse des An-
fordernden, so ist auch diese Prüfung erfolgreich durch- 60
geführt. Dann wird das aktuelle Datum und die aktuelle Uhrzeit in den nächsten beiden Schritten mit den Daten BENDAT und BENDAU im dekodierten Schlüssel ver-
glichen. Ist auch hier Übereinstimmung gegeben, wird der Prozeß für den anfordernden Benutzer freigegeben. 65
Ist irgendeine der beschriebenen Prüfungen nicht er-
füllt, wird der anfordernde Benutzer zurückgewiesen.

Patentansprüche

1. Verfahren zur Überprüfung der Zugangsberech-
tigung des Benutzers eines Datenverarbeitungsnet-
zes zu einem daran angeschlossenen Prozeß unter
Benutzung eines Passwortes, dadurch gekenn-
zeichnet, daß im Datenverarbeitungsnetz ein Au-
thentifizierungsrechner (ATH) vorgesehen ist, zu
dem ein den Zugang zu einem Prozeß anfordernder
Benutzer mit ihm zugeordneten bestimmten Pass-
wort Zugang erhält, daß der Authentifizierungs-
rechner bei Anforderung eines bestimmten Prozes-
ses durch den Benutzer einen Schlüssel (SL) er-
zeugt, daß der Schlüssel (SL) eine Benutzermaske
(BENMAS) enthält, die angibt, zu welchen der an
das Datenverarbeitungsnetz angeschlossenen Pro-
zesse der anfordernde Benutzer eine Zugangsbe-
rechtigung hat, daß dieser Schlüssel an den anfor-
dernden Benutzer zurückübertragen wird, und daß
der Benutzer unter Verwendung dieses Schlüssels
den von ihm gewünschten Prozeß ansteuert, daß
dann in dem Prozeß die Benutzermaske (BEN-
MAS) aus dem Schlüssel (SL) und aus der Benut-
zermaske (BENMAS) die Zugangsberechtigung
des anfordernden Benutzers festgestellt und, falls
vorhanden, diesem der Zugang zu dem Prozeß frei-
gegeben wird.

2. Verfahren nach Anspruch 1, dadurch gekenn-
zeichnet, daß der Schlüssel (SL) zusätzlich zur Be-
rechtigungsmaske (BENMAS) die Netzadresse
(NETADR) des anfordernden Benutzers enthält.

3. Verfahren nach Anspruch 1 oder 2, dadurch ge-
kennzeichnet, daß der Schlüssel zusätzlich das Da-
tum (BENDAT) und die Dauer (BENDAU) der Zu-
gangsberechtigung enthält.

4. Verfahren nach Anspruch 1 oder einem der fol-
genden, dadurch gekennzeichnet, daß der Schlüssel
(SL) im Authentifizierungsrechner (ATH) kodiert
(KSL) wird.

Hierzu 3 Seite(n) Zeichnungen

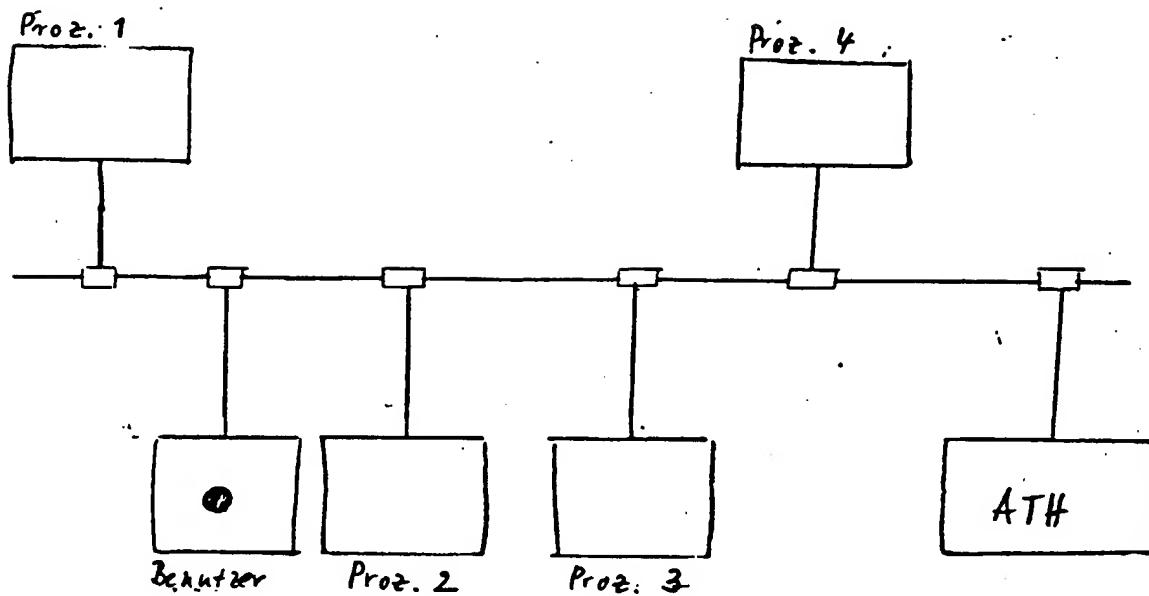


Fig. 1

		Prozesse				
		1	2	3	4	
Benutzer	A	0	1	1	0	usw.
	B	1	1	0	0	usw.

BENMAS

Fig. 2

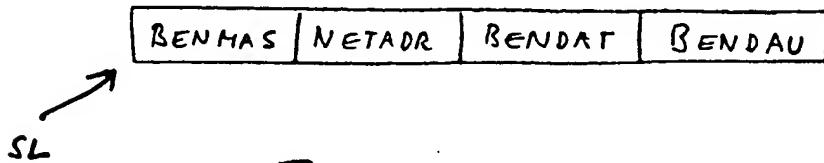


Fig. 3

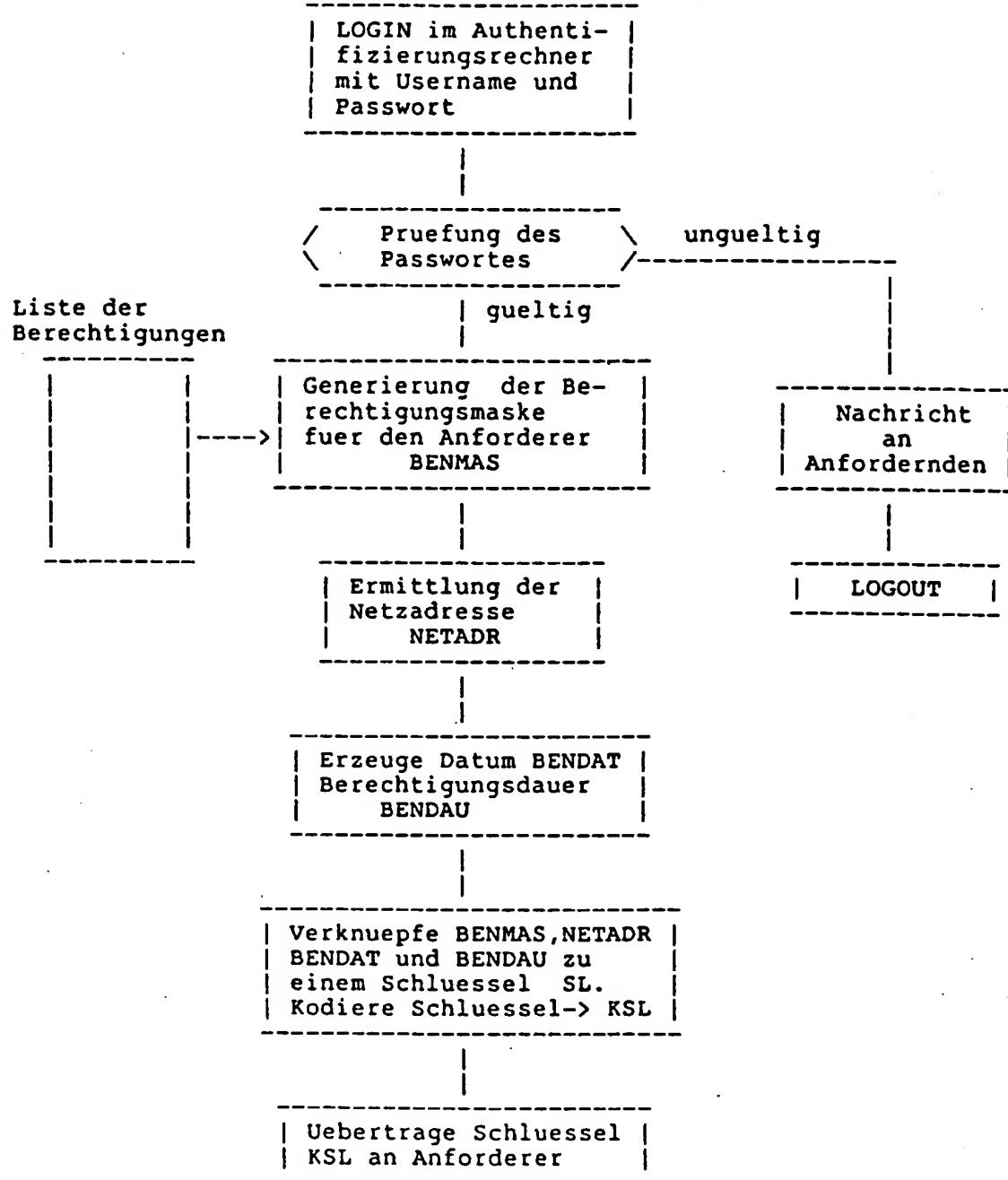


Fig. 4

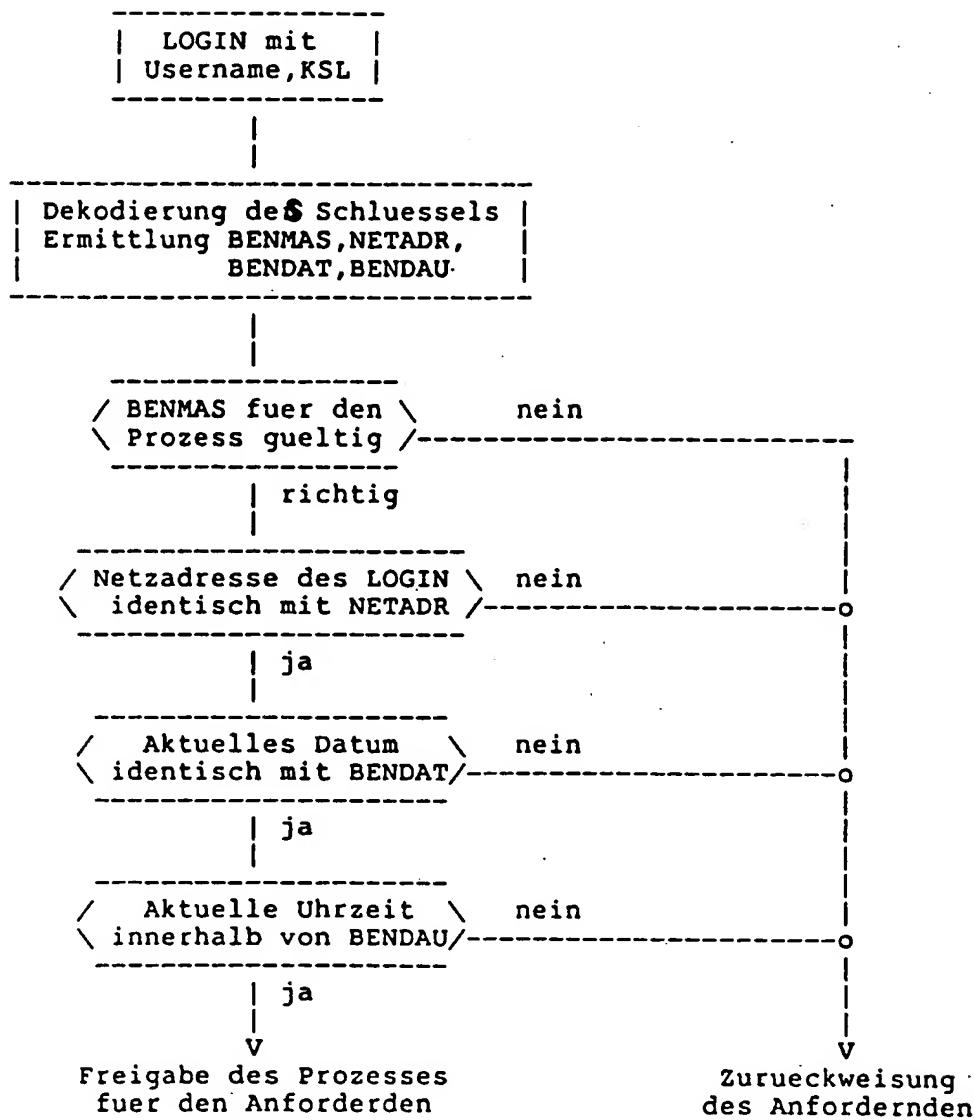


Fig. 5

[First Hit](#) [Previous Doc](#) [Next Doc](#) [Go to Doc#](#)

End of Result Set

[Generate Collection](#) [Print](#)

L1: Entry 1 of 1

File: DWPI

Oct 2, 1991

DERWENT-ACC-NO: 1991-296641

DERWENT-WEEK: 199603

COPYRIGHT 2004 DERWENT INFORMATION LTD

TITLE: User password identification for data processing network access - generating multiple-parameter key from single password per user to enable access to many routines

INVENTOR: MARTIN, G

PATENT-ASSIGNEE:

ASSIGNEE	CODE
STANDARD ELEKTRIK LORENZ AG	INTT
ALCATEL SEL AG	ALCAN

PRIORITY-DATA: 1990DE-4010094 (March 29, 1990)

[Search Selected](#) [Search ALL](#) [Clear](#)

PATENT FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
Search Results DE 4010094 A	October 2, 1991		000	
User Searches DE 4010094 C2	December 14, 1995		006	G06F012/14

Preferences

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
DE 4010094A	March 29, 1990	1990DE-4010094	
DE 4010094C2	March 29, 1990	1990DE-4010094	

INT-CL (IPC): G06F 12/14

ABSTRACTED-PUB-NO: DE 4010094A

BASIC-ABSTRACT:

The data processing network contains a password identification unit. Upon entry of a password, a user is allocated a unique 'key' which determines access limits to the network and may be constructed of the following parameters: a mask defining routines to which access is allowed, user network location, entry date, permitted access duration. The identification unit may also encode the 'key' for added security.

ADVANTAGE - Single password per user for entering several processes. Ease of central password management without affecting network routines. Password identifier

and 'key' generator protected from tampering. Unused passwords can be set to expire automatically.

ABSTRACTED-PUB-NO:

DE 4010094C

EQUIVALENT-ABSTRACTS:

The data processing network contains a password identification unit. Upon entry of a password, a user is allocated a unique 'key' which determines access limits to the network and may be constructed of the following parameters: a mask defining routines to which access is allowed, user network location, entry date, permitted access duration. The identification unit may also encode the 'key' for added security.

ADVANTAGE - Single password per user for entering several processes. Ease of central password management without affecting network routines. Password identifier and 'key' generator protected from tampering. Unused passwords can be set to expire automatically.

CHOSEN-DRAWING: Dwg.1/5 Dwg.1/5

TITLE-TERMS: USER PASSWORD IDENTIFY DATA PROCESS NETWORK ACCESS GENERATE MULTIPLE PARAMETER KEY SINGLE PASSWORD PER USER ENABLE ACCESS ROUTINE

DERWENT-CLASS: T01 W01

EPI-CODES: T01-H01C; W01-A06;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N1991-227268

[Previous Doc](#)

[Next Doc](#)

[Go to Doc#](#)

This Page is inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT OR DRAWING
- BLURED OR ILLEGIBLE TEXT OR DRAWING
- SKEWED/SLANTED IMAGES
- COLORED OR BLACK AND WHITE PHOTOGRAPHS
- GRAY SCALE DOCUMENTS
- LINES OR MARKS ON ORIGINAL DOCUMENT
- REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images
problems checked, please do not report the
problems to the IFW Image Problem Mailbox